

**Appln No. 10/083,236**  
**Amdt date December 11, 2007**  
**Reply to Office action of October 19, 2007**

**REMARKS/ARGUMENTS**

Claims 1, 3-23, and 25-38 are pending. Claims 1 and 22 are amended and new claim 38 is added.

Applicant thanks the Examiner for his time for the telephonic interview conducted on December 4, 2007.

Claims 1, 3-23 and 25-37 are rejected under 35 U.S.C 112, first paragraph, as failing to comply with the written description requirement. More specifically, the Office action states that "the specification does not support execution of command or any description that distinguishes execution of commands from performing operations." While the Applicant agrees that the specification does not support any description that distinguishes execution of commands from performing operations, the support for executing commands is provided on page 60, lines 22-24 and 28-30 of the specification. As a result, it is respectfully requested that the above rejections be withdrawn.

Claims 1, 3-23 and 25-37 are rejected under 35 U.S.C 103(a) as being unpatentable over Cordery (U.S. 6,466,921) and further in view of Lewis (U.S. 6,233,565). Applicant submit that all of the pending claims are patentable over the cited references, and reconsideration and allowance of the pending claims are respectfully requested.

The claimed invention is directed to a system and method for providing public key infrastructure security in a computer network. The system includes a remote database for securely storing a user transaction data record for each user and a remote cryptographic device. Each user transaction data record includes few operational states. For example, a "Raw state," an "Unleased" state, an "Assigned state," and a "Leased state." (See, for example, specification page 60, line 16 to page 61, line 16.). Moreover, only a predetermined type of commands (operations) are allowed to be executed on the user transaction data record for each predetermined state. (Page 59, lines 12-15; page 60, lines 22-24, and 27-29). The cryptographic

**Appln No. 10/083,236**  
**Amdt date December 11, 2007**  
**Reply to Office action of October 19, 2007**

device executes one or more of the commands that are allowed for a present state of the user transaction data record. (Page 59, lines 12-15; and page 60, line 16 to page 61, line 16.). This adds another layer of security to the database records that are already encrypted.

The cryptographic device may also include different states (a finite state machine), wherein only a predetermined type of commands are executed by the cryptographic device for each state. (Page 41).

More particularly, the amended independent claim 1 includes, among other limitations "wherein the user transaction data record includes a raw state, an unleased state, an assigned state and a leased state, and a data element indicating a present operational state of the user transaction data record including one of the raw state, the unleased state, the assigned state and the leased state, wherein only a predetermined type of commands are allowed to be executed on the user transaction data record for each operational state" and "a cryptographic device . . . to encrypt and decrypt the data in the user transaction data record . . . , and to execute one or more of the commands that are allowed for the present state of the user transaction data record." None of the cited references, alone or in combination, teach or suggest the above limitations.

Cordery describes a Database Server 36 where the information is securely stored using secure cryptographic processes. (FIG. 1 and col. 6, lines 36-40). Each meter record in the database Server 36 includes account information, meter freshness data and other postal information. (Col. 7, lines 27-34 and 38-41). According to Cordery, this freshness data is "data that is unique for each transaction." Moreover, "the meter box compares freshness data that is stored in meter box for each meter account to freshness data stored as part of the meter record. (Col. 9, lines 49-54, emphasis added.). In Cordery's system "if the compared freshness data are not identical, then, at step 230, the meter box ends the transaction and alerts the Function Server 34 for possible tampering." (Col. 9, lines 59-62, emphasis added.).

Therefore, even assuming that this freshness data can be construed as a "state" of the data record, Cordery does not teach or suggest "a raw state, an unleased state, an assigned state, and a

**Appln No. 10/083,236**  
**Amdt date December 11, 2007**  
**Reply to Office action of October 19, 2007**

leased state" for the data record. Furthermore, Cordery does not teach or suggest "execute[ing] one or more of the commands that are allowed for the present state of the user transaction data record," because as shown in the cited FIG. 4, if the comparison data is not identical (block 225), the transaction is ended and no command can be executed (block 230).

Lewis in the cited text describes a "Finite State Machine" for the "Client Cryptographic Module," which includes different states. (See, col. 22, line 33, and col. 23, line 65). These different states of the "Client Cryptographic Module" are not the same as the state of the user transaction data, rather, they are the states of the hardware module ("Finite State Machine" for the "Client Cryptographic Module"). More importantly, Lewis, alone or in combination with Cordery, does not disclose or suggest "a raw state, an unleased state, an assigned state, and a leased state" for the data record.

As a result, amended independent claim 1 is patentable over the combination of Cordery and Lewis.

Amended independent claim 22 includes, similar limitations and therefore it is also patentable over the combination of Cordery and Lewis.

New independent claim 38 includes among other limitations "wherein the user transaction data record includes a data element indicating three or more predetermined operational states for the user transaction data record, wherein only a predetermined type of commands are allowed to be executed on the user transaction data record for each predetermined operational state," "a cryptographic device . . . for executing one or more of the commands that are allowed for a present state of the user transaction data record," and "wherein the cryptographic device includes three or more states, wherein only a predetermined type of commands are executed by the cryptographic device for each state."

As the Examiner correctly states, Cordery does not teach "a data element indicating three or more predetermined operational states for the user transaction data record." Additionally, as

**Appln No. 10/083,236**  
**Amdt date December 11, 2007**  
**Reply to Office action of October 19, 2007**

explained above, Cordery does not teach or suggest "executing one or more of the commands that are allowed for a present state of the user transaction data record," because as shown in the cited FIG. 4, if the comparison data is not identical (block 225), the transaction is ended and no command can be executed (block 230) for that (present) state.

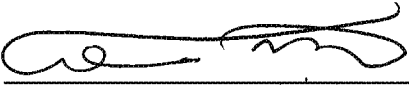
However, the Examiner cites col. 23 line 64 to col. 25 line 60 of Lewis as teaching the limitation of "three or more predetermined operational states for the user transaction data record." Applicant respectfully disagree. As explained above, these cited states of Lewis are the states of a "Finite State Machine" for the "Client Cryptographic Module," which includes different states. (See, col. 22, line 33, and col. 23, line 65). Therefore, these different states of the "Client Cryptographic Module" are not the same as the state of the user transaction data. Rather, they are the states of the hardware module ("Finite State Machine" for the "Client Cryptographic Module") similar to the claimed cryptographic device including "three or more states, and wherein only a predetermined type of commands are executed by the cryptographic device for each state.," in claim 38.

In short, the independent claims 1 22, and 38 define a novel and non-obvious invention over the cited references. The remaining dependent claims 3-21, 23, and 25-37 are dependent from claims 1 and 22, respectively and therefore include all the limitations of their respective independent claims and additional limitations therein. Accordingly, these claims are also allowable over the cited references, as being dependent from allowable independent claims and for the additional limitations they include therein.

**Appln No. 10/083,236**  
**Amdt date December 11, 2007**  
**Reply to Office action of October 19, 2007**

In view of the foregoing remarks and amendments, it is respectfully submitted that this application is now in condition for allowance, and accordingly, reconsideration and allowance are respectfully requested.

Respectfully submitted,  
CHRISTIE, PARKER & HALE, LLP

By   
Raymond R. Tabandeh  
Reg. No. 43,945  
626/795-9900

RRT/clv

CLV PAS768850.1-\* -12/11/07 10:19 AM